REMARKS

No claims have been amended, added, or canceled. Therefore, claims 1-6, 8-31, 33-47 and 49-72 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 102(a) Rejection:

The Final Office Action rejected claims 1-6, 8-15, 17-22, 24-31, 33-37, 41-47, 49-55 and 57-72 under 35 U.S.C. § 102(a) as being clearly anticipated by Czerwinski, et ál., "An Architecture for a Secure Service Discovery Service" (hereinafter, "Czerwinski").

Regarding claim 1, Czerwinski fails to disclose binding the client capabilities to the authentication credential. In contrast, Czerwinski teaches two separate mechanisms for authentication credentials and capabilities, respectively. Specifically, Czerwinski discloses a Certificate Authority responsible for providing authentication certificates and a separate Capability Manager that generates and distributes capabilities. Under Czerwinski's system, a client contacts a Capability Manager to obtain a capability credential that is later used when sending a query to discover services. The SDS server is responsible for matching a client's query with service descriptions and uses the client's capabilities to ensure that only those services to which the client is granted access are returned to the client. Additionally, a client in Czerwinski's system separately contacts the Certificate Authority to obtain an authentication credential (Czerwinski, sections 3.1, 3.4, and 3.1 paragraph 5). Nowhere does Czerwinski describe binding the capabilities obtained from the Capability Manager with the authentication credential obtained from the Certificate Authority.

In response the Applicants arguments above, the Examiner, in the Response to Arguments section of the Final Office Action, states "Czerwinski discloses the CM generates the capability after authentication so that the SDS can perform access control based on the capabilities sent by client" and further states, "the capabilities received by the client from CM is actually the authentication credential." The Examiner's interpretation of Czerwinski is incorrect. Czerwinski specifically states, "[c]apability distribution itself can be done *without authentication* because capabilities, like certificates, are securely associated with a single principal, and only the clients possessing the appropriate private key can use them" (emphasis added, Czerwinski, section 3.4, paragraph 3). Thus, contrary to the Examiner's assertion, a client in Czerwinski's system is not authenticated before receiving a capability. A capability may be associated with a client, without being bound to any authentication credential. Furthermore, the capabilities received by the clients are not authentication credentials, also contrary to the Examiner's assertion.

For at least the reasons presented above, the rejection of claim 1 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 1 apply to claim 62.

Regarding claim 3, contrary to the Examiner's assertion, Czerwinski does not teach wherein said advertisement for said first service includes <u>a data representation language schema *defining a message interface* for accessing</u> said first service. In contrast, Czerwinski discloses domain advertisements that contain "the multicast address to use for sending service announcements, the desired service announcement rate, and contact information for the Certificate Authority and the Capability Manager" (Czerwinski, section 3.1, paragraph 1). Additionally, Czerwinski's service descriptions contain service metadata, such as location, required capabilities, time-out period, and JAVA RMI addresses (Czerwinski, section 2.3, paragraph 3). Neither the domain advertisements nor the service descriptions of Czerwinski include <u>a data representation language schema defining a message interface</u> for accessing a service.

The Examiner cites a portion of Czerwinski (section 3.1) that describes how a client submits a query in the form of an XML template. However, a client query using an XML template as the content of a query is very different from a data representation language schema defining <u>a message interface</u> for accessing a service. The XML template in a client query in Czerwinski does not define a message interface for accessing a service. Instead client queries include desired services and are matched against service descriptions to find services providing those desired services (Czerwinski, section 2.3, paragraph 3 and section 3.1, paragraph 5). Further, Czerwinski teaches the use of Authenticated Remote Method Invocation (ARMI) for communication between client applications and SDS servers, *and it is well known that ARMI uses Java interface classes, and not data representation language schemas*, to define the methods that are exposed for remote calling. Thus, Czerwinski clearly fails to teach wherein the advertisement for the first service includes a data representation language schema defining a message interface for accessing the first service.

In response the Applicants arguments above, the Examiner argues, "Czerwinski discloses that a client submits a query in the form of an XML template so that the SDS can use the form to perform service (sic) for the client" and further contends, "the XML template is a data representation language schema to define a interface for the service to perform tasks." Applicants strongly disagree. Firstly, the Examiner appears to be ignoring the specific wording of Applicants' claim. Claim 3 recites, in part, a data representation language schema defining a *message* interface for accessing a service. The Examiner has neglected to cite any passage of Czerwinski that discloses a data representation language schema defining a message interface. The Examiner refers to a query in XML, which Czerwinski describes as including such factors as, "cost, performance, location, and device- or service-specific capabilities" (Czerwinski, Abstract). As is readily apparent from Figure 2 of Czerwinski, a client query is not a data representation schema, and clearly does not define a message interface for accessing a service. Furthermore, there is no way for a client to define such a message interface in a query template when the client has not even located a service (that is purpose of submitting the query template). It would be impossible for the client to define a message interface for a service that has not even been located and/or selected.

Thus, the rejection of claim 3 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 3 apply to claims 14, 18, 29, 37, 44, 53, 59, 64 and 70.

Regarding claim 17, contrary to the Examiner's assertion, Czerwinski fails to teach said client generating a message gate for accessing said first service, wherein said message gate embeds said authentication credential in *every* message from said client to said first service. The Examiner has cited sections 3.1, 3.3 and 3.4 of Czerwinski that describe the working of the SDS server, Certificate Authority, and Capability Manager of Czerwinski's system. However, neither the Examiner's cited passage, nor any other portion of Czerwinski, discloses generating a message gate for access the first service, wherein the message gate embeds the authentication credential in every message from the client to the first service. In contrast, Czerwinski teaches the use of Authenticated Remote Method Invocation (ARMI) for communication between client applications and SDS servers. Czerwinski also teaches that ARMI uses certificates to authenticate each of the endpoints and states that such authentication consists of a short handshake to establish a symmetric key used for the rest of the session. (Czerwinski, section 3.5.3, paragraph 2). After the certificate-based authentication at the start of an ARMI session, only the session encryption key is used to validate the remaining messages of the ARMI session. No certificate or credential is embedded with every message of an ARMI session. Thus, Czerwinski fails to teach embedding the authentication credential in every message from the client to the service.

In response the above arguments, the Examiner, in the Response to Arguments section of the Final Office Action, states, "Czerwinski discloses that when the client sends a query to the SDS server, the client include[s] the client's capabilities." However, as noted above, Czerwinski teaches that capabilities are distributed without authentication (Czerwinski, section 3.4, paragraph 3). Also, Czerwinski's system also specifically includes a Certificate Authority responsible for generating authentication certificates, which are different than capabilities. Thus, Czerwinski's capabilities are clearly not authentication credentials. A client submitting a query to an SDS service and including the client's capabilities does not involve or imply embedding an authentication credential in every message.

Furthermore, the Examiner has failed to rebut Applicants' argument regarding Czerwinski's use of ARMI and that ARMI messaging does not include embedding an authentication credential in every message.

Thus, the rejection of claim 17 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 17 apply to claims 58 and 69.

Regarding claim 27, Czerwinski fails to teach a *client device* configured to determine client capabilities for the client, wherein the client capabilities are capabilities of the service device that said client is permitted to use, and further fails to teach a *client device* configured to bind the client capabilities to the authentication credential. Instead, as discussed above, Czerwinski teaches two separate mechanisms for authentication credentials and capabilities. Specifically, Czerwinski discloses a Certificate Authority responsible for providing authentication certificates and a separate Capability Manager that generates and distributes capabilities. None of the clients described by Czerwinski are configured to determine capabilities for a client and bind those capabilities to an authentication credential. The Capability Manager then generates capability credentials that are supplied by clients when querying the SDS server to find services. The SDS server ensures that only those services that the client is allowed to discover, based on the client's capability credential, are returned to the client. (Czerwinski, sections 3.1, 3.4, and section 3.1, paragraph 5). Czerwinski does not mention anything about a client device configured to determine client capabilities for the client, wherein the client capabilities are capabilities of the service device that the client is permitted to use and further fails to mention a client device configured to bind the client capabilities to the authentication credential.

For at least the reasons given above, the rejection of claim 27 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 27 apply to claim 51.

Regarding claim 43, Czerwinski fails to teach a *service device* configured to determine client capabilities for the client, wherein the client capabilities are capabilities of the service device that the client is permitted to use, and also fails to teach a *service device* configured to bind the client capabilities to the authentication credential. Instead, as described above, Czerwinski teaches two separate mechanisms for authentication credentials and capabilities. Specifically, Czerwinski discloses a Certificate Authority responsible for providing authentication certificates and a separate Capability Manager that generates and distributes capabilities. None of the services described by Czerwinski are configured to determine capabilities for a client and bind those capabilities to an authentication credential. Instead services in Czerwinski's system contact the Capability Manager and specify those principals, such as clients, that are allowed to discover and access that service. Thus, each of Czerwinski's services supplies an access control list (ACL) to the Capability manager. The Capability Manager then generates and distributes capability credentials that are supplied by clients when querying an SDS server to find services. The SDS server ensures that only those services that the client is allowed to discover, based on the client's capabilities, are returned to the client. (Czerwinski, sections 3.1, 3.4, and section 3.1, paragraph 5). Czerwinski does not mention anything about a *service device* configured to determine client capabilities for the client, wherein the client capabilities are capabilities of the service device that the client is permitted to use, and further fails to mention a *service device* configured to bind the client capabilities to the authentication credential.

Thus, the rejection of claim 43 is not supported by the prior art and its removal is respectfully requested. Similar remarks as discussed above in regard to claim 43 apply to claims 58 and 59.

Section 103(a) Rejection:

The Final Office Action rejected claims 16, 23, 38, 39 and 56 under 35 U.S.C. § 103(a) as being unpatentable over Czerwinski in view of Johnson et al. (U.S. Patent 5,560,008), and claim 40 as being unpatentable over Czerwinski in view of Applicant's Applied Prior Art. Applicants traverse these rejections for at least the reasons given above in regard to the respective independent claims.

In regard to the rejections under both sections 102(a) and 103(a), Applicants also assert that numerous ones of the dependent claims recite further distinctions over the cited art. However, since the rejection has been shown to be unsupported for the independent claims, a further discussion of the dependent claims is not necessary at this time.

Information Disclosure Statement:

Applicants note that an information disclosure statement with accompanying Form PTO-1449 was submitted on February 8, 2005. Applicants request the Examiner to carefully consider the listed references and return a copy of the signed and initialed Form PTO-1449 from this statement.

CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above referenced application from becoming abandoned, Applicants hereby petition for such an extension. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5181-64800/RCK.

Also enclosed herewith are the following items:

☒ Return Receipt Postcard

□ Petition for Extension of Time

□ Notice of Change of Address

□ Fee Authorization Form authorizing a deposit account debit in the amount of $ for fees ( ).

□ Other:

Respectfully submitted,

Robert C. Kowert
Reg. No. 39,255
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: April 22, 2005